UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,455	03/31/2004	Robert W. Seaton JR.	16222U-014110US	8400

66945 7590 01/22/2008

TOWNSEND AND TOWNSEND CREW LLP
TWO EMBARCADERO CENTER, 8TH FLOOR
SAN FRANCISCO, CA 94111

EXAMINER	
GEE, JASON KAI YIN	
ART UNIT	**PAPER NUMBER**
2134	

MAIL DATE	DELIVERY MODE
01/22/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/816,455	SEATON ET AL.	
	Examiner	Art Unit	
	Jason K. Gee	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 November 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 10-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 10-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/07/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is response to communication: amendment filed on 11/07/2007.

2. Claims 1-8, 10-34 are currently pending in this application. Claims 33 and 34 are new. Claims 1, 16, 18, 19, 28, and 32 are independent claims.

3. The IDS received 11/07/2007 has been accepted. The Applicant has cited many difference references on the IDS, and if he knows any particular reference that stands out more than the others, he should notify the Examiner.

Response to Arguments

4. Applicant's arguments with respect to the claims regarding the ACS requesting a passcode has been considered but are moot in view of the new ground(s) of rejection. Although the Hodgson reference still applies, the reference is interpreted differently to teach the limitations of the claims.

5. Applicant's arguments with respect claim 18 regarding a destination address has been considered but are moot in view of the new ground(s) of rejection.

6. Applicant's arguments filed in regards to the limitations of the previous claim 9 now incorporated into the independent claims have been fully considered but they are not persuasive.

The appellants also argue the limitations of claim 9, which are now incorporated into the limitations of claim 1. However, Hodgson teaches this throughout the reference as well. It was already indicated in the previous reference that the PIN is encrypted, as

described in paragraph 154. The appellant argues that this PIN is not encrypted as it is entered in the front end HSM. However, this is not persuasive. Hodgson teaches throughout the reference that the PIN is never in the clear (paragraphs 92 and73). Further, Hodgson teaches many different inputs regarding the PIN in paragraph 58. The PIN/passcode may be entered in through a magnetic card, a smart card (inherently includes encryption), or even biometric data (inherently encrypted). Further, paragraph 59 teaches additional security regarding the PIN/PAD.

Even further, as seen in light of claim 29 of the claims, the front end HSM comprises the back end HSM. As can be seen throughout the reference, such as in paragraphs 30, the HSM does indeed receive an encrypted PIN, decrypts, and reencrypts it. The HSM as described in paragraph 30 matches the front and back end HSM as taught in light of the applicants claims and specification.

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 1-17, 19, 20, 22-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Hodgson et al. US Patent Application Publication 2002/0123972 (hereinafter Hodgson).

As per claim 1, 6, and 9, Hodgson teaches a secure passcode authentication system, the system comprising: An Access Control Server (ACS) configured to receive a request for passcode authentication of a Primary Account Number (PAN), and configured to request a passcode corresponding to the PAN (Figure 1, paragraph 62, 34, 72; wherein the ACS is the merchant server and the STMS 30 and 20,22); a front end Hardware Security Module (HSM) coupled to the ACS, and configured to receive the passcode in an encrypted format and generate an encrypted passcode using a local encryption key (paragraph 58, 59, 73, 92, 154, Figure 1); a back end HSM configured to receive the encrypted passcode from the front end HSM and further configured to recover a clear form of the passcode, generate a back end encrypted passcode, and communicate the back end encrypted passcode to an authentication network, wherein the system authenticates the passcode (pargraph 30, 57, 61, 76-80, and paragraphs 151-154 and figure 1; a security zone password is used between the front and back end HSM, and another password is used between the HSM and the authentication network, as seen in paragraphs 151-154 and throughout the reference).

As per claim 2, Hodgson teaches a secure passcode authentication system, wherein teh request for passcode authentication comprises a request for a personal identification number authentication (paragraph 19, and taught throughout the reference).

As per claim 3, Hodgson teaches wherein the ACS is further configured to receive an authentication message from the authentication network (paragraph 90 and Figures 2a-2c).

As per claim 4, Hodgson teaches a secure passcode authentication system, wherein the ACS is further configured to generate a unique transaction identification and include the unique transaction identification as a hidden field in the request for the passcode (paragraph 98, lines 5-7, and Figure 2c).

As per claim 5, Hodgson teaches a secure apsscode authentication system, wherein the front end HSM is configured to generate a hash value based in part on the unique transaction identification, and wherein the ACS is configured to include the hash values as an additional hidden ifled in the request for the passcode (paragraph 27, 90 and 154).

As per claim 7, Hodgson teaches a secure passcode authentication system, wherein the front end HSM comprises a software HSM (paragraph 23).

As per claim 8, Hodgson teaches a secure passcode authentication system, wherein the front end HSM comprises a hardware HSM (paragraph 23).

As per claim 10, 22-24, and 30, Hodgson teaches a secure passcode authentication system, whereint eh first encrypted format comprises a SSL encrypted format (paragraph 76).

As per claim 12, Hodgson teaches a secure passcode authentication system, wherein the front end HSM is configured to receive a cardholder encrypted passcode

from a cardholder device (paragraph 19, pin/pad is corresponding to a cardholder device).

As per claim 13, Hodgson teaches a secure passcode authentication system, where the back end HSM is configured to generate the back end encrypted passcode by generating a PINBLOCK using the clear form of the passcode and encrypting the PINBLOCK using an Acquirer Working Key (Paragrah73, DES or ATM).

As per claim 14, Hodgson teaches a secure passcode authentication system, wherein the authentication network comprises an Internet Payment Gateway Server (paragraph 66 and 99, where IPGS corresponds to STS-MF which is inside of the merchant server).

As per claim 15, Hodgson teaches a secure passcode authentication system, whereint eh authentication network further comprises an issuer server coupled to the IPGS (paragraphs 60).

As per claim 16, 20, 31, and 32, Hodgson teaches a secure passcode authentication system, the system comprising: an access control server configured to receive a request for PIN authentication of a PAN, and configured to generate a requ3est for a PIN corresponding to the PAN (paragraph 62, and as rejected in claim1), the request for the pin including hidden fields comprising a unique transaction identifier and a hash value (paragraph 27, 90, 154, and as rejected in the previous claims), a front end HSM coupled to the ACS (paragraph 154, Figure 1), and configured to generate the hash value based in part on the unique transaction identifier (paragraph

27, 90, 154), and further configured to receive an encrypted PIN, decrypt the PIN to recover a clear form of the PIN (paragraph 30), and generate a local encrypted PIN using a local encryption key (paragraph 154), and a back end HSM configured to receive the local encrypted PIN from the front end HSM and further configured to recover a clear form of the PIN from the local encrypted PIN (paragraph 57, 61, 11-14, Figure 1A), generate an AWK encrypted PIN, and communicate the AWK encrypted PIN to an authentication network (paragraph 73).

As per claim 17, Hodgson teaches a secure passcode authentication system, wherein the front end HSM generates the local encrypted key using a triple DES algorithm (paragraph 154).

As per claims 19, 27, and 28, Hodgson teaches a method for providing secure passcode authentication, the method comprising:

Requesting a PIN corresponding to a PAN (paragraph 62 and as rejected in the previous independent claims); receiving the encrypted PIN in a front end HSM in response to the request (paragraph 62), generating a PINBLOCK based in part on the encrypted PIN (paragraph 73), encrypting the PINBLOCK using a local key in the front end HSM to generate a local key encrypted PINBLOCK (paraggraph 73); decrypting the local key encrypted PINBLOCK with a back end HSM (paragraph 3), generating a back end encrypted PIN with the back end HSM (paragraph 57); communicating the back end encrypted PIN to an authentication network (Figure 1, throughout the reference);

and receiving an authentication response from the authentication network (paragraph 90, Figures 2A-2C)..

As per claim 26, Hodgson teaches a method for providing secure passcode authentication, wherein encrypting the PINBLOCK comprises encrypting the PINBLOCK using a triple DES encryption algorithm (paragraph 26).

As per claim 29, Hodgson teaches a method for providing a secure passcode authentication, wherein the fron end HSM comprises the back end HSM (paragraph 57).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 18, 21, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hodgson as applied above, and in view of Morrill, Jr. US Patent No. 5,991,749 (hereinafter Morrill).

Claim 18 is rejected using the same basis of arguments used to reject claims 1 and 16 above. However, at the time of the invention, Hodgson does not explicitly teach wherein the request for the PIN includes an instruction to provide the PIN to a destination address. However, this would have been obvious, if not even inherent. Hodgson already teaches that the PIN is routed to STMS or POS processors, and it would be obvious that this would go to a particular address (it has to go somewhere!).

This is shown in paragraph 153, where PIN information is forwarded to an address. However, for argument's sake Morrill teaches wherein a request for a PIN explicitly indicates an address (Morill col. 2 line 60 to col. 3 line 5).

At the time of the invention, it would have been obvious to one of ordinary skill in the art to combine the Morill and Hodgson references. One of ordinary skill in the art would have been motivated to perform such an addition to allow the PIN to be sent to a particular address, and not just an arbitrary address. Doing so would provide more safety, as a PIN would not be sent to a random area. Although Morill teaches telecommunications, this may be incorporated into Hodgsons, as taught in paragraph 153.

As per claim 21, generating a query having an instruction direct a query response be directed to a destination address corresponding to the front end HSM, and communicating the query over an Internet connection to a cardholder device, is taught by the combination of Hodsons and Morrill as applied above in claim 18. Hodsons teaches the addresses are over internet connections and that the PIN's are forwarded to the correct destination addresses.

As per claim 34, Hodgson teaches throughout the reference that addresses are HTTP addresses, such as seen in the rejections above, and throughout the reference. These addresses would direct the PIN number and bank payment information to be redirected to the websites assocaited with the POS's and the STMS.

9. Claim 33 is rejected under 35 U.S.C. 103(a) as being obvoius over Hodgson as applied above.

As per claim 33, it would have been obvious, if not inherent to Hodgson, to have a directory server to verify a PAN's eligibility to participate in secure passcode authentication. As can be seen in Figure 6-10, only authorized type of cards may be used. If the type of card is not authorized, the transaction would not be completed. Also, in dealing with ATMS, a personal account number may not be able to participate if the account number is expired or other reasons, which would be obvious. Further, as well known and practiced in the art, only eligible users are allowed to participate in special services such as banking transactions, to ensure security and efficiency.

At the time of the invention, it would have been obvious to one of ordinary skill in the art to determine whether an account number is eligible to participate in a secure passcode authentication. One of ordinary skill in the art would have been motivated to perform such an addition to selectively allow approved users to use the system. Bank accounts or credit cards that are not approved should not be allowed to particpate as it would only waste resources. Verifying whether an account number is eligible allows only authorized users to access the system that would be beneficial to them. Doing so would create more efficiency and create more security.

Conclusion

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jason K. Gee whose telephone number is (571) 272-6431. The examiner can normally be reached on M-F, 7:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jason Gee
Patent Examiner
Technology Center 2100
01/08/2008

KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER